UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

NICHOLAS NELLI, *on behalf of himself and all others similarly situated,* Plaintiff, v. AT&T INC., Defendant.	Case No.: 3:24-cv-00759 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Nicholas Nelli ("Plaintiff") brings this Class Action Complaint against AT&T Inc. ("AT&T" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated current and former customers' ("Class Members," defined *infra*) sensitive information, including full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, and AT&T account numbers and passcodes ("personally identifiable information" or "PII").[1]

[1] Aimee Ortiz, *AT&T Resets Millions of Passcodes After Customer Records Are Leaked*, THE NEW YORK TIMES (Mar. 30, 2024), https://www.nytimes.com/2024/03/30/business/att-passcodes-reset-data-breach.html (last visited Mar. 30, 2024) (citing Zack Whittaker, *AT&T resets account passcodes after millions of customer records leak online*, TechCrunch (Mar. 30, 2024), https://techcrunch.com/2024/03/30/att-reset-account-passcodes-customer-data/).

2. AT&T is a multinational telecommunications corporation and, with its subsidiaries and affiliates, is one of the United States's most popular wireless carriers and Internet providers.

3. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

4. As a result of a cybersecurity incident ("Data Breach"), the PII of Plaintiff and approximately 73 million Class Members, including 7.6 million current AT&T customers and 65.4 million former AT&T customers, was exfiltrated.[2] AT&T has stated the data set "appears to be from 2019 or earlier."[3] Moreover, the notice emails AT&T sent to affected customers on March 30, 2024 ("Notice Emails") state, "It appears the data is from more than 4 years ago."[4]

5. AT&T admitted in the Notice Emails that the affected data included full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, and AT&T account numbers and passcodes.[5]

6. In 2021, a hacker claiming the Data Breach posted a small sample of records, but it was difficult to determine if the posted data was authentic.[6] In March 2024, a data seller published the full 73 million records on a known cybercrime forum.[7] On March 30, 2024, AT&T first acknowledged publicly that the leaked data is authentic.[8]

---

[2] *Id*
[3] *Id*.
[4] Associated Press, *AT&T Notifies Users of Data Breach and Resets Millions of Passcodes*, U.S. NEWS & WORLD REPORT (Mar. 30, 2024) https://www.usnews.com/news/us/articles/2024-03-30/at-t-notifies-users-of-data-breach-and-resets-millions-of-passcodes (last visited Mar. 30, 2024).
[5] *Id*.
[6] Zack Whittaker, *AT&T resets account passcodes after millions of customer records leak online*, TechCrunch (Mar. 30, 2024), https://techcrunch.com/2024/03/30/att-reset-account-passcodes-customer-data/).
[7] *Id*
[8] *Id*.

7. Defendant failed to adequately protect Plaintiff's and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its clients' customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents; and (iii) notify Plaintiff and Class Members within a reasonable time after their PII was compromised. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of

the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII.

11. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

12. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C.§ 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs, and the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C.§ 1332(d)(2)(A).

14. The Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in this District.

15. Venue is proper under 28 U.S.C § 1391 because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

16. Plaintiff Nicholas Nelli is a natural person and resident and citizen of the state of Georgia, residing in Woodstock, Cherokee County, Georgia, where he intends to remain.

17. Defendant AT&T Inc. is a corporation organized under the state laws of Delaware with its headquarters and principal place of business located in Dallas, Texas.

FACTUAL ALLEGATIONS

Defendant's Business

18. AT&T is a multinational private telecommunications corporation that sells wireless and Internet services.[9]

19. Plaintiff and Class Members are current and former customers at Defendant, in a data set apparently stolen circa 2019, who provided their PII to Defendant as a condition of obtaining services.[10]

20. The information held by AT&T in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

21. Upon information and belief, AT&T made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining services would be kept safe, confidential, that the privacy of that information would be maintained, and that AT&T would delete any sensitive information after they were no longer required to maintain it.

22. Indeed, AT&T provides on its Privacy Notice on its website that:

> We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit

[9]

[10] *Supra* n.1.

> access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information.[11]

23. Plaintiff and Class Members provided their PII to AT&T with the reasonable expectation and on the mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of AT&T to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

25. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant had a legal duty to keep consumer's PII safe and confidential.

26. Defendant had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

27. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services they provide.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

[11] AT&T Privacy Notice, https://about.att.com/privacy/privacy-notice.html (last visited Mar. 30, 2024).

The Data Breach

29. In or about March 2024, the PII of 73 million former and current AT&T customer accounts, including those of 7.6 million current customers and 65.4 million former customers, were published online on a known cybercrime forum.[12]

30. The leak was first publicly revealed in 2021, but there was no way to authenticate it coming from AT&T directly.[13] "Details of the leaked data first appeared online in August 2021, when a known threat actor, ShinyHunters, offered up the records for sale on a hacking forum, with a 'buy it now' price of one million dollars."[14] In March 2024, "that same data appears to have been made available for free by another threat actor, MajorNelson."[15]

31. AT&T's website now states the following:

> It has come to our attention that a number of AT&T passcodes have been compromised. We are reaching out to all 7.6M impacted customers and have reset their passcodes. In addition we will be communicating with current and former account holders with compromised sensitive personal information.
>
> Our internal teams are working with external cybersecurity experts to analyze the situation. To the best of our knowledge, the compromised data appears to be from 2019 or earlier and does not contain personal financial information or call history.
>
> We encourage customers to remain vigilant by monitoring account activity and credit reports. You can set up free fraud alerts from nationwide credit bureaus—Equifax, Experian, and TransUnion. You can also request and review your free credit report at any time via Freecreditreport.com.[16]

---

[12] *Supra* n.1.
[13] *Id.*
[14] Jack Turner, *70 Million AT&T Accounts Leaked Online – How to Check Yours*, TECH.CO (Mar. 23, 2024), https://tech.co/news/att-accounts-leaked-70-million-check#:~:text=AT%26T%20Customer%20Data%20for%20Sale&text=Details%20of%20the%20leaked%20data,price%20of%20one%20million%20dollars.
[15] *Id.*
[16] *Keeping your account secure*, AT&T, https://www.att.com/support/article/my-account/000101995/ (last visited Mar. 31, 2024).

32. Thus, AT&T has admitted the Data Breach likely occurred in 2019, but is only now (5 years later) reaching out to affected customers. Instead of providing them even with free credit monitoring routinely provided in a data breach, AT&T passes all the costs onto affected customers (Plaintiff and Class Members) and instructs them to "remain vigilant by monitoring their account activity and credit reports." This is egregiously insufficient.

33. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

34. The attacker accessed and acquired files containing unencrypted PII of Plaintiff and Class Members, including their full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, and AT&T account numbers and passcodes. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

35. As the data set was apparently stolen in 2019, and was first known to the public in 2021, AT&T waited an inexcusable 3 to 5 years until they were forced to by the threat actor's publication of the PII, to take responsibility for the breach.

Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of PII Are Particularly Suspectable to Cyber Attacks.

36. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, even preceding 2019.

37. Data thieves regularly target telecommunications companies like Defendant due to the highly sensitive information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally

monetize that PII through unauthorized access.

38. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

39. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

40. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

41. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

42. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

43. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

44. As corporation in possession of their customers' and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

45. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[18]

46. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[19]

47. For example, PII can be sold at a price ranging from $40 to $200.[20] Criminals can

[17] 17 C.F.R. § 248.201 (2013).
[18] *Id.*
[19] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Mar. 30, 2024).
[20] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 30, 2024).

also purchase access to entire company data breaches from $900 to $4,500.[21]

48. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names and Social Security numbers.

49. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[22]

50. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

51. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

---

[21] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Mar. 30, 2024).

[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Mar. 30, 2024).

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited Mar. 30, 2024).

Defendant Failed to Comply with FTC Guidelines.

52. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

53. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

55. The FTC has brought enforcement actions against businesses for failing to

adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

56. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of their data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

57. Defendant was at all times fully aware of its obligation to protect the PII of customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

58. As noted above, experts studying cybersecurity routinely identify institutions as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

59. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include but are not limited to: educating all customers, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which customers can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

60. Other best cybersecurity practices that are standard at large institutions that store

PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

61. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

62. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendant Breached Its Duties to Safeguard Plaintiff's and Class Members' PII.

63. In addition to its obligations under federal and state laws, Defendant owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of Class Members.

64. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above; and

f. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

65. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

66. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

Common Injuries & Damages

67. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion

of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft.

68. Plaintiff and Class Members have been since the Data Breach, and are still, at a heightened risk of identity theft, which will continue for their lifetimes.

69. Unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

70. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

71. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

72. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and

trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

73. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

74. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

75. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

76. The existence and prevalence of "Fullz" packages means that the PII stolen from

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Mar. 30, 2024).

the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

77. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

78. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft and Fraud

79. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

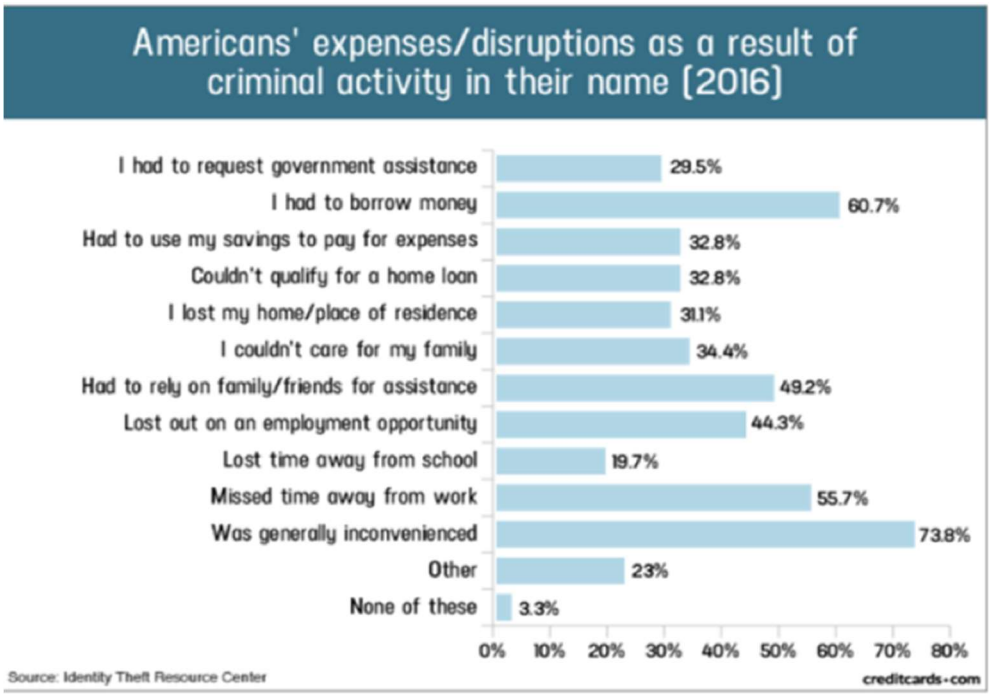
80. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

81. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and

credit record."[25]

82. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[26]

83. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[27]



[25] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[26] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Mar. 30, 2024).

[27] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Mar. 30, 2024).

84. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

Diminution Value Of PII

85. PII is a valuable property right.[29] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

86. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[30]

87. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[31,32]

88. Consumers who agree to provide their web browsing her tory to the Nielsen Corporation can receive up to $50.00 a year.[33]

---

[28] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. GOV'T ACCOUNTABILITY OFFICE, June 2007, https://www.gao.gov/ new.items/d07737.pdf (last visited Mar. 30, 2024) ("GAO Report").

[29] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[30] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Mar. 30, 2024).

[31] https://datacoup.com/ (last visited Mar. 30, 2024).

[32] https://digi.me/what-is-digime/ (last visited Mar. 30, 2024).

[33] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Mar. 30, 2024).

89. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[34]

90. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

91. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names and Social Security numbers.

92. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

93. The fraudulent activity resulting from the Data Breach may not come to light for years.

94. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Mar. 30, 2024).

95. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network, amounting to thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

96. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.

97. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

98. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

99. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for their lifetimes.

100. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class

Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Citrix's failure to safeguard their PII.

Plaintiff's Experience

101. Plaintiff Nicholas Nelli is a resident of Woodstock, Georgia, where he intends to remain.

102. He has been an AT&T customer since 2012, and has had a family wireless account continuously since then, and also uses AT&T for his TV and Internet.

103. On March 30, 2024, he received an email from AT&T stating: "We have discovered that your AT&T account passcode has been compromised, therefore we have proactively reset your passcode."

104. The email went on to state: "Our internal teams are working with external cybersecurity experts to analyze the situation. It appears the data is from more than 4 years ago and does not contain personal financial information or call history . . . The information varied by customer and account, but may have included full name, email address, mailing address, phone number, social security number, date of birth, AT&T account number and passcode."

105. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to AT&T had he known of AT&T's lax data security policies.

106. Plaintiff suffered and will suffer actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) lost or diminished value of his PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the

Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as AT&T fail to undertake appropriate and adequate measures to protect the PII.

107. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

108. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for his lifetime.

109. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

110. Plaintiff brings this class action individually on behalf of himself and on behalf of all members of the following classes of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Class:

> All persons residing in the United States whose PII was compromised in the Data Breach, including all who were sent a notice email of the Data Breach.

111. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s)

112. Plaintiff reserves the right to modify or amend the foregoing Class definition

before the Court determines whether certification is appropriate

113. Numerosity: Class Members are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, it has been reported that approximately 73 million individuals' information was exposed in the Data Breach.

114. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiff's and Class Members' PII violated the FTC Act and/or state laws, and/or Defendants' other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

g. Whether Plaintiff and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

h. Whether an implied contract existed between Class Members and Defendant with respect to protecting PII and privacy, and whether that contract was breached;

i. Whether Plaintiff and Class Members are entitled to credit or identity monitoring and monetary relief; and

j. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

115. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

116. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed Class Members, had his PII compromised in the Data Breach. Plaintiff and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all class members.

117. Adequacy: Plaintiff will fairly and adequately protect the interests of Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this

nature.

118. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for class members to individually seek redress from Defendant's wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

119. Injunctive and Declaratory Relief: Defendant has acted and/or refused to act on grounds generally applicable to the class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the class as a whole.

120. All proposed Class Members are readily ascertainable. Defendant has access to the names in combination with mailing addresses and/or email addresses of class members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent Notice Email.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

121. Plaintiff incorporates paragraphs 1 through 120, as if fully set forth herein.

122. Plaintiff and Class Members entrusted their PII to AT&T as a condition of obtaining services.

123. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

124. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with industry standards concerning data security would result in the compromise of that PII—as in the Data Breach that occurred. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

125. Moreover, Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

126. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to class members' PII;

d. Failing to detect in a timely manner that class members' PII had been compromised;

e. Failing to remove former employees' PII they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

127. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered or will imminently suffer damages, as set forth in the preceding paragraphs.

128. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

129. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

130. Defendant's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' PII in an unsafe and insecure manner.

131. Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates paragraphs 1 through 120, as if fully set forth herein.

133. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

134. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and Class Members' sensitive PII.

135. Defendant violated its duties under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable

consequences of a data breach, including, specifically, the immense damages that would result to customers in the event of a data breach, which ultimately came to pass.

136. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

137. Defendant had a duty to Plaintiff and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Class's PII.

138. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII/PII.

139. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

140. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

141. The injury and harm suffered by Plaintiff and Class Members were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and Class Members to suffer the foreseeable harms associated with the exposure of their PII.

142. Had Plaintiff and Class Members known that Defendant did not adequately protect their PII, Plaintiff and Class Members would not have entrusted Defendant with their PII.

143. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the actual misuse of

their compromised PII; (ii) invasion of privacy; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

COUNT III
BREACH OF AN IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

144. Plaintiff incorporates paragraphs 1 through 120, as if fully set forth herein.

145. Defendant offered to provide services to Plaintiff and Class Members in exchange for payment and PII.

146. In turn, and through internal policies described in the preceding paragraphs, and other conduct and representations, Defendant agreed it would not disclose the PII it collects to unauthorized persons and that it would safeguard customer PII.

147. Plaintiff and Class Members accepted Defendant's offer by providing PII to Defendant and paying money to Defendant.

148. Implicit in the parties' agreement was that Defendant would adequately safeguard the PII of Plaintiff and Class Members and would provide them with prompt and adequate notice of all unauthorized access and/or theft of their PII.

149. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

150. Defendant materially breached the contract(s) it had entered into with Plaintiff and

Class Members by failing to safeguard their PII, and by failing to notify them promptly of the Data Breach that compromised such information. Defendant further breached the implied contracts with Plaintiff and Class Members by:

a. Failing to properly safeguard and protect Plaintiff's and Class Members' PII;

b. Failing to comply with industry standards, as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to properly supervise its agents in possession of PII;

d. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

151. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

152. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

153. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

154. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

155. Defendant failed to advise Plaintiff and Class Members of the Data Breach promptly and sufficiently.

156. In these and other ways, Defendant violated its duty of good faith and fair dealing.

157. Plaintiff and Class Members have sustained injury-in-fact and damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

158. Plaintiff incorporates paragraphs 1 through 120, as if fully set forth herein.

159. This claim is pleaded as the alternative to the breach of implied contract claim.

160. Plaintiff and Class Members conferred a benefit upon Defendant in the form of purchasing services, and by providing their PII to Defendant as a condition of obtaining services.

161. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

162. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the services they received with reasonable data privacy and security practices and procedures, and the services they received without unreasonable data privacy and security practices and procedures.

163. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class Members' payment and their PII because Defendant failed to adequately protect their PII. Plaintiff and Class Members would not have provided their PII, nor paid Defendant for services, had they known Defendant would not adequately protect their PII.

164. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct and the Data Breach alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Nicholas Nelli, individually, and on behalf of all others similarly situated, requests that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: March 31, 2024

Respectfully submitted,

By: */s/ Bruce W. Steckler*
Bruce W. Steckler, TX Bar No. 00785039
STECKLER WAYNE & LOVE, PLLC
12720 Hillcrest Road, Suite 1045
Dallas, TX 75230
Tel: (972) 387-4040
Fax: (972) 387-4041
bruce@swclaw.com

Jeff Ostrow (*pro hac vice* forthcoming)
Steven Sukert (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: 954-525-4100
ostrow@kolawyers.com

Gary Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

J. Gerard Stranch, IV (*pro hac vice* forthcoming)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com

Counsel for Plaintiff and the Putative Class